(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 093 525**
A1

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: 83302114.0

(22) Date of filing: 14.04.83

(51) Int. Cl.³: H 04 L 9/02
H 04 K 1/02

(30) Priority: 30.04.82 GB 8212623

(43) Date of publication of application:
09.11.83 Bulletin 83/45

(84) Designated Contracting States:
AT BE CH DE FR GB IT LI LU NL SE

(71) Applicant: BRITISH TELECOMMUNICATIONS
2-12 Gresham Street
London EC2V 7AG(GB)

(72) Inventor: Serpell, Stephen Charles
35 Elhurst Drive
Ipswich IP3 0PB(GB)

(72) Inventor: Brookson, Charles Bile
21 Meadowvale Close
Ipswich IP4 4HE(GB)

(72) Inventor: Gordon, John Asley
18 Roe Green Close
Hatfield Hertfordshire(GB)

(72) Inventor: King, Graham Kenneth
13 Gibbons Close Sandridge
St. Albans Hertfordshire(GB)

(74) Representative: Smith, Norman Ian et al,
F.J. CLEVELAND & COMPANY 40-43 Chancery Lane
London WC2A 1JQ(GB)

(54) **Broadcasting encrypted signals.**

(57) Binary signals for broadcasting are encrypted by a pseudorandom bit-stream generated from a secret key and an initialisation bit-stream. The initialisation stream is multiplexed, broadcast, recovered at the receiver and used to regenerate the pseudorandom stream for decrypting. The multiplexing ensures synchronisation.

Each pseudorandomiser, at transmitter and receiver, has a ciphering engine 11 containing the key 10. 64-bit words are pseudorandomised and fed back from output register 13, and the pseudorandomised words are sent bit-by-bit on line 15 as the encryption stream. Random number generator 16 produces an initialisation stream which is formed into words by initialisation register 17 and periodically transferred to input register 12 by control codes from unit 22.

Control codes, on line 17, and initialisation stream, on line 18, are multiplexed and broadcast. Each receiver separates the control pulses and initialisation stream whereby register 17 obtains initialisation words and microprocessor 11 regenerates the description stream.

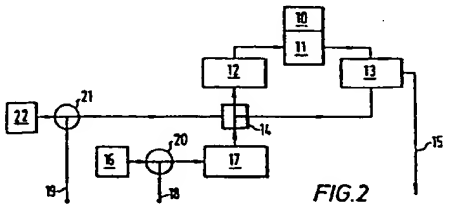

FIG.2

EP 0 093 525 A1

BROADCASTING ENCRYPTED SIGNALS

DESCRIPTION

This invention relates to the transmission of encrypted signals.

Telecommunications, e.g. speech, data, video, facsimile, have been transmitted over closed networks so that eavesdropping has been very difficult. It is now proposed to use satellite radio links in which signals are broadcast over wide areas, e.g. the whole of Europe. In these circumstances eavesdropping is so simple that there is a danger of unacceptable loss of privacy. To restore privacy it is intended to encrypt signals in such broadcast channels. More specifically it is intended to encrypt the signals using the "Data Encryption Standard" described in "FIPS PUB 46" of National Bureau of Standards of Department of Commerce of US Government. To facilitate understanding of this invention it is convenient to provide a brief description of the "output feedback mode" as described

in "FIPS PUB 81". The publication defines an algorithm which has as data a key and an input work both of 64 bits. From these two items of data the algorithm produces a pseudorandomised output word of 64 bits. (In the K-bit output feedback mode the K most significant bits of the "output word" are exclusively ORed with K bits of the message to be encrypted. The next "input word" is formed by discarding the most significant K bits of the last "input word", shifting the remaining bits K positions to the left, and then inserting the K output bits first used into the least significant bit positions). Thus in the 64-bit output feedback mode there is a chain in which the nth output word becomes the (n + 1)th input word. In order to start the chain it is necessary to provide the key (which is fixed throughout the chain) and the first input word; it is convenient to call this first input word the "initialisation vector" or "IV". The algorithm described in "Data Encryption Standard" (FIPS PUB 46) is generally known as the DES algorithm.

When used as described above, the output feedback mode generates a very long pseudorandom bit-stream. This bit-stream is used to encipher a binary signal by pairing its bits with the bits of the pseudorancom

bit-stream and operating with "exclusive or" on each pair. Decrypting is carried out by repeating the encrypting process. Thus the recipient generates the same pseudorandom stream, reforms the same pairs and repeats the "exclusive or". It is essential to obtain exact synchronisation and this causes practical problems in the use of this mode of the DES algorithm.

The DES algorithm has been used in telecommunications in output feedback mode and synchronisation has been achieved by "handshake" procedures. These require two-way communication and it is now desired to extend the use of the algorithms so that it can be used in one-way systems. It is also intended to use satellite systems wherein there are a plurality of receivers for one transmitter. In such circumstances handshake procedures become complicated and cumbersome or even impractical. In a one-way system the number of receivers is not important.

According to this invention one-way transmission of encrypted signals is achieved by generating the pseudorandom bit-stream from an initialisation bit stream and time multiplexing the initialisation stream with the encrypted signal. At the receiver the initialisation stream is demultiplexed and used to generate the same pseudorandom stream as at the

transmitter. The pseudorandomiser for generating the pseudorandom stream preferably includes an initialisation register for assembling the initialisation stream into initialisation vectors. As specified in the appended claims the invention includes the following aspects:

1 a method of transmission

2 a method of reception

3 a pseudorandomiser

4 a transmitter, and

5 a receiver.

One embodiment of the invention will now be described by way of example with reference to the accompanying drawings in which:-

Figure 1 illustrates the structure of a time-multiplex frame for use in the invention;

Figure 2 illustrates a pseudorandomiser according to the invention;

Figure 3 illustrates a transmitter according to the invention, and

Figure 4 illustrates a receiver according to the invention.

The method according to the invention applies digital encryption to a binary digital signal, which may be inherently digital, e.g. data transmission, or coded analogue, e.g. speech, video or facsimile. Time multiplexing is used for binary coded speech and the frame structure used is shown in Figure 1.

Each frame consists of sixty-four time slots of which sixty are used for communication and four are used for system and cryptographic purposes. Slots 0, 16 and 48 are used conventionally, i.e. slot 0 contains a fixed bit-pattern which enables the receiver to identify the start of each frame and slots 16 and 48 contain conventional signal information, e.g. ending or starting of traffic in specified slots. Slot 32 contains cryptographic as well as conventional framing information. The remaining slots, i.e. slots 1 to 15, slots 17 to 31, slots 33 to 47 and slots 49 to 63 contain a signal encrypted by a pseudorandom bit-stream. The generation of this stream will now be described; the pseudorandomiser used is illustrated in Figure 2.

The pseudorandomiser shown in Figure 2 is based on a conventional usage described in "FIPS PUB 81" as the "output feedback mode". The apparatus comprises an encryption engine 11 containing a key 10. This

receives an input word from an input register 12 and generates, using the DES algorithm, a pseudorandom first output word which is placed in an output register 13. The first output word is fed-back to the input register 12 via a switch 14 which is actuated by an initiation control unit 22. In addition to this feed-back the word in the output register 13 is also sent out, bit-by-bit, on the cypher output line 15. From the input register 12, the first output word passes through the encryption engine to generate a pseudorandomised second output word in the output register 13. The feed-back continues and thereby generates a chain of pseudorandomised words each of which is output, bit-by-bit, on the cypher output line 15; this output constitutes the pseudorandom bit-stream used for encryption. To initiate the chain it is necessary to provide an initial word in register 12; the initial word is called an "initialisation vector" or "IV". The DES algorithm is capable of generating very long pseudorandom bit-strings from a single IV and long chains are usually used. The present method departs from this practice by frequently loading new initialisation vectors and thus uses rather short chains, preferably 512 output words long. The chains restart at frequent intervals, e.g.

about 100 microseconds to 10 seconds depending on the rate of transmission.

To achieve this restart the pseudorandomiser shown in Figure 2 includes an initialisation stream generator 16, preferably a true random number generator, which supplies an initialisation bit-stream to an IV register 17 which assembles the initialisation stream into an IV. The restart is effected by control unit 22 which at suitable intervals, e.g. every 512 words in the feed-back chain, transmits an input code to switch 14. This interrupts the feed-back from output register 13 to register 12 and transfers the IV in IV register 17 to input register 12. It will be apparent that each transfer starts a new chain with a new IV.

The initialisation stream (from generator 16) is also sent to transmission via initialisation lead 18 and the input code (from control unit 13) is also sent to transmission via control lead 19. Referring back to Figure 1, the initialisation stream and control pulses are multiplexed in slot 32.

At the receiver there is an indentical arrangement having mode switches 20 and 21 reversed to give a receive mode. The initialisation stream is taken from slot 32 and supplied, via mode switch 20,

to IV register 17 where it is assembled into the same IV as at the transmitter. The input codes are also taken from slot 32 and supplied, via mode switch 21, to the switch 14, so that IV's, identical to those at the transmitter, are transferred to the input register 12 thereby operating an identical pseudorandom bit-stream or cypher output line 15. It is imperative that bit-streams are synchronised at transmitter and receiver. This is achieved according to the invention because the initialisation stream and control codes are multiplexed into a composite signal with a frame structure.

As shown in Figure 3 a transmitter according to the invention includes a pseudorandomiser 30 which is as shown in Figure 2 with mode switches 20 and 21 (as shown) in the "transmit" position.

The transmitter accepts a binary signal, e.g. multiplexed binary coded speech, on lead 31. This signal passes first to an "exclusive or" gate 32 where it is combined with the pseudorandom bit-string on line 15, and then to a multiplexer 33 where the initialisation stream (on line 18) is placed in slot 32 together with the restart code (on line 19). The composite signal thus produced passes to transmitter 34 and it is radiated (to a satellite) by aerial 35.

After broadcasting by the satellite the composite signal is received by the receiver shown in Figure 4. This also includes a pseudorandomiser 40 which is as shown in Figure 2 with mode switches 20 and 21 (as shown) in the "receiver position" (in which initialisation stream generator 16 and the control unit 22 are disconnected).

As shown in Figure 4, an aerial 41 picks up the composite signal and passes it to a receiver 42 and thence to a formatter 43 which recognises the sync-code in slot 0 and hence organises the signal into its frame. After formatting the signal passes to demultiplexer 44 which separates the initialisation stream from slot 32 and sends it, via line 18 and mode switch 20, to IV register 17. The demultiplexer 44 also separates the control pulses from slot 32 and sends them, via line 19 and mode switch 21, to switch 14.

The signal then passes to an "exclusive or" gate 45 where it is combined with the pseudorandom bit-stream on line 15. This decrypts the signal which continues for conventional processing, e.g. further demultiplexing.

The overall operation of the transmitter and receiver is as follows:-

As preparation the same key is placed in pseudorandomisers 30 and 40. The keys are provided by seucure transport. For example a large number of keys are recorded and conveyed by messenger to the transmitter and receivers; this makes it convenient to change the key every 24 hours. It is essential to have the same key at all stations. The key is the only "secret" element in the system.

Under control of the key the pseudorandomiser 30 produces a pseudorandom bit-stream which is applied to the signal by "exclusive or" gate 32. The initialisation stream, from which the pseudorandom stream is generated, is multiplexed with the signal and so are the control codes which indicate the use of a new IV.

At each receiver the control stream is separated by demultiplexer 44 and assembled in IV register 17 into the same IV as at the transmitter. The control codes, also demultiplexed from the composite signal, initiate the use of a new IV at the same time as at the transmitter so each pseudorandomiser 40 generates the same pseudorandom bit-stream which decrypts the signal at "exclusive or" gate 45. It is emphasised that the encryption and decryption do not depend on

the nature of the multiplexing since the multiplexed signal is treated as a string of bits. Thus it is possible to use different forms of multiplex from time to time as the nature of the traffic charges. For speech it is convenient to multiplex 30 channels, i.e. slot "n" carries the same channel as slot "n + 32". At higher information rates, e.g. video or data, it is convenient for all slots to carry the same channel.

The most important advantages of the invention are:-

i achievement of synchronisation of the pseudorandomiser streams at transmit and receiver ends of a link without recourse to a return channel (broadcast or unidirectional application) since the system continuously transmits IVs and instructions about when to load them;

ii achievement of a system wherein any loss of pseudorandomiser synchronisation (due to transmission faults, bit losses, or transmission interruptions of any duration) is speedily and automatically corrected because each time the system loads a new IV it effectively resynchronises the pseudorandomisers anew; and

iii achievement of a system wherein a new receiver can join in a communication irrespective of how long the communication has already been in progress, i.e. simultaneous start-ups of transmitters and receivers is not required (important in a broadcast system wherein the operator could not shut everything down and restart every time a new receiver is brought on-line, maybe months after commencement of transmission).

CLAIMS

1. A method of transmitting a binary digital signal in encrypted form which comprises:-

a. generating a pseudorandom bit-stream

b. combining an input signal with the pseudorandom bit-stream to produce an encrypted signal

characterised in that the pseudorandom bit-stream is generated from a fixed key and an initialisation bit-stream and the initialisation stream is time multiplexed with the encrypted signal to produce a composite signal which is transmitted.

2. A method of transmitting a binary digital signal as claimed in claim 1 wherein the combining step is carried out by pairing the bits of the signal with the bits of a pseudorandom stream and operating with "exclusive or" on each pair.

3. A method of receiving and decrypting a composite signal produced as claimed in claim 1 or claim 2 wherein the original pseudorandom bit-stream is reproduced from the same fixed key and recombined with the encrypted signal to produce the decrypted signal, characterised in that the initialisation bit-stream is demultiplexed from the composite signal and used to regenerate the pseudorandom bit-stream.

4. Pseudorandomiser for generating a pseudorandom bit-stream which comprises a ciphering engine (11) having an input register (12) and an output register (13), said ciphering engine (11) being adapted to accept the content of the input register (12) and to produce therefrom a pseudorandomised word in the output register (13), wherein the apparatus also includes output means (15) for producing the content of the output register as a pseudorandom bit-stream and feedback means for transferring the content of the output register to the input register (12), characterised in that the pseudorandomiser also includes an initialisation register (17) for forming an initialisation bit-stream into input words and transfer means (14) for transferring the content of

the initialisation register (17) into the input register on receipt of an input code.

5. Pseudorandomiser according to claim 4 characterised in that it also includes a random number generator (16) for generating the initialisation bit-stream and control means (22) for periodically producing the input code.

6. A transmitter for carrying out a method according to claim 1 characterised in that it includes a pseudorandomiser (30) according to claim 5 and a combining means (32) for receiving a binary input signal, said combining means (32) being connected to the output means of the pseudorandomiser whereby the input signal is encrypted, the transmitter also comprising a multiplexer (33) connected to the random number generator and a multiplexer (33) connected to the control means whereby the initialisation stream and the control codes are multiplexed with the encrypted input signal to produce a composite signal.

7. A transmitter according to claim 6 wherein the combining means (32) is an "exclusive or" gate.

8. A receiver for carrying out a method according to claim 3 characterised in that it includes a pseudorandomiser (40) according to claim 4 and a demultiplexer (44) for separating the initialisation bit-stream from the composite signal, said demultiplexer being connected to the initialisation register (17) of the pseudorandomiser; wherein the receiver also comprises a demultiplexer (44) for separating the control codes from the composite signal and applying each of said control codes to transfer the content of the initialisation register (17) to the input register (12) of the pseudorandomiser whereby the pseudorandomiser generates the same pseudorandom bit-stream as the transmitter and wherein the receiver also comprises combining means (45) for receiving the encrypted signal, said combining means (45) being connected to the output means of the pseudorandomiser whereby the decrypted signal is produced.

9. A receiver according to claim 8 wherein the combining means (45) is an "exclusive or" gate.

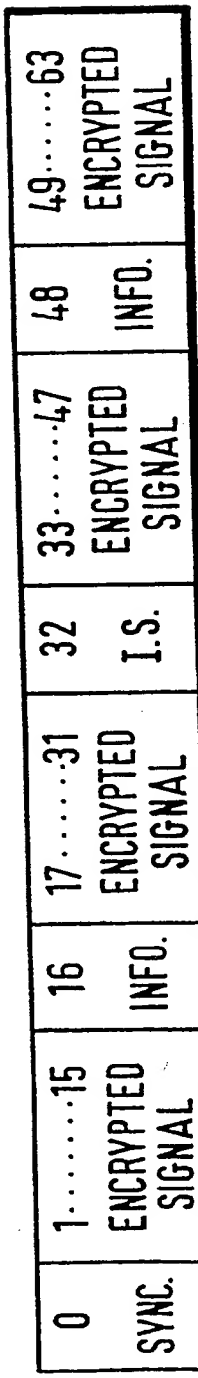
0
SYNC.
1.....15
ENCRYPTED SIGNAL
16
INFO.
17.....31
ENCRYPTED SIGNAL
32
I.S.
33.....47
ENCRYPTED SIGNAL
48
INFO.
49.....63
ENCRYPTED SIGNAL

FIG.1

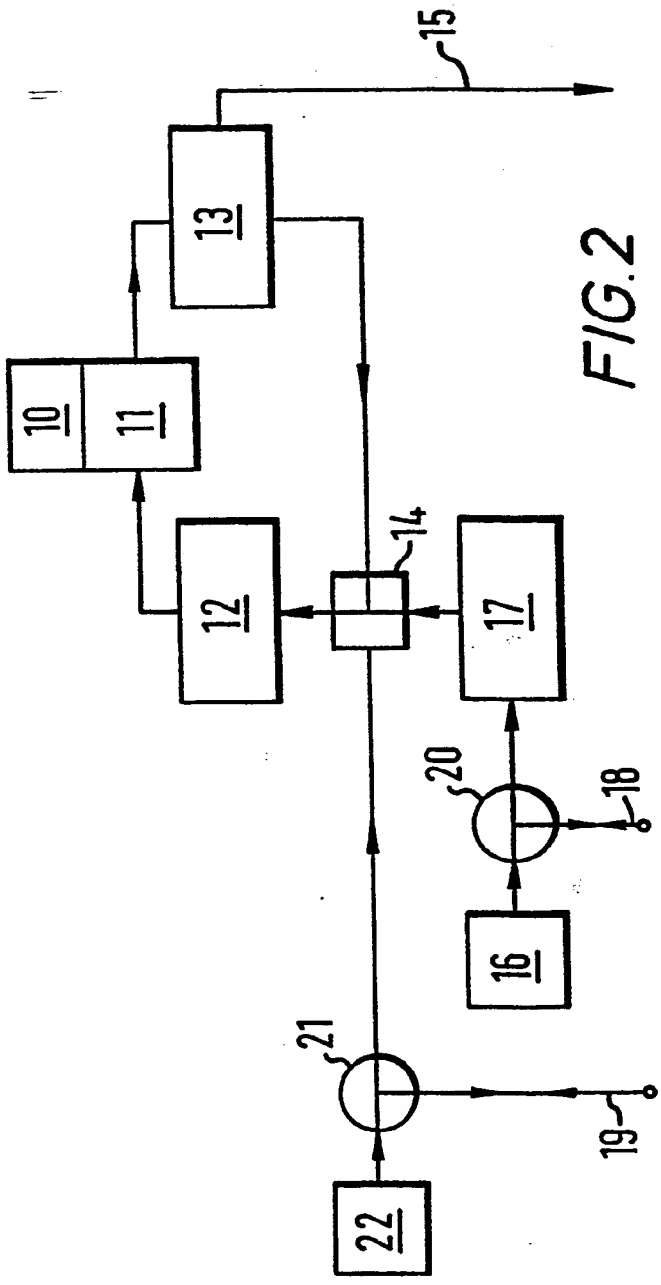
15
13
10
11
12
14
17
20
18
16
21
19
22

FIG.2

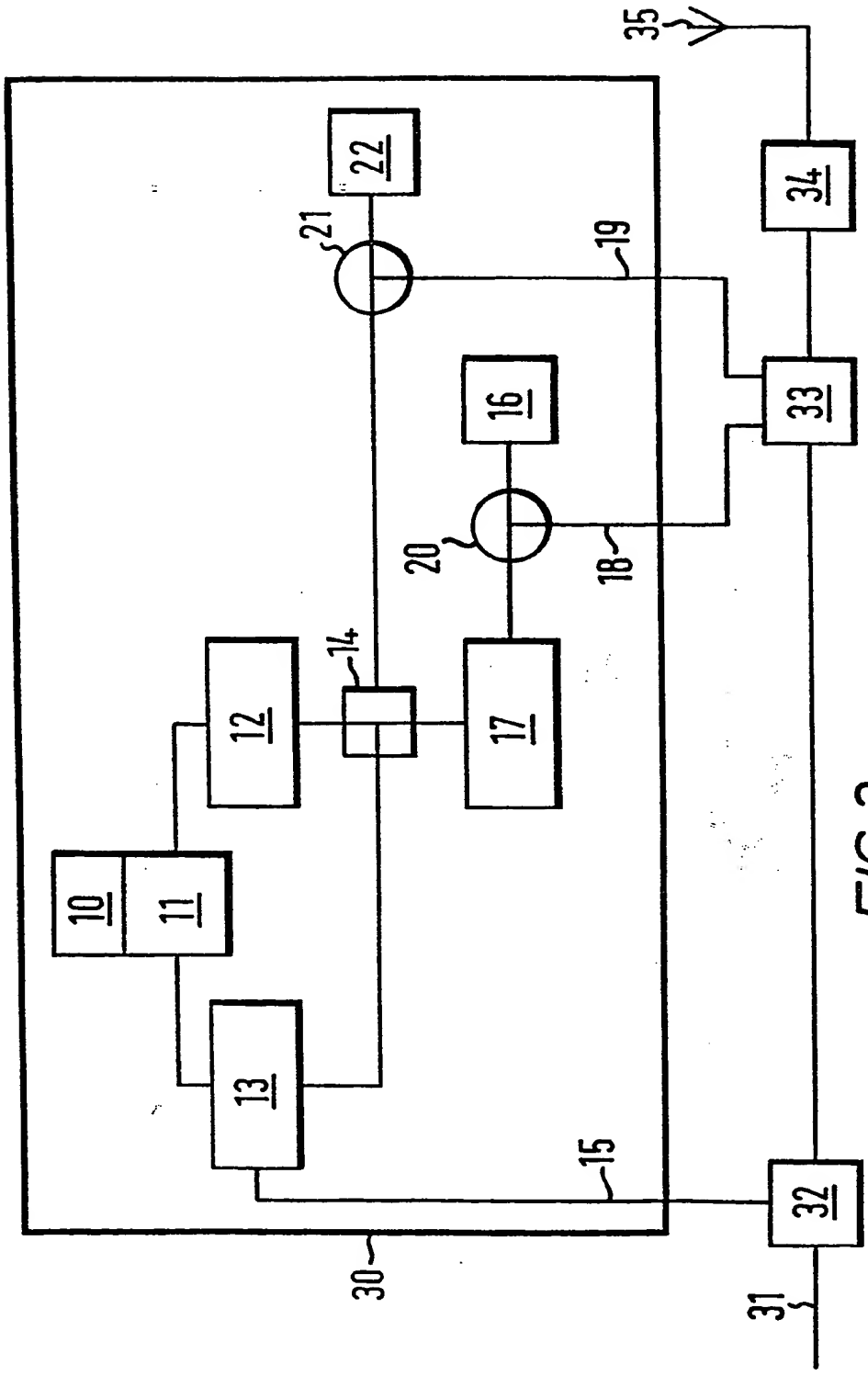

FIG.3

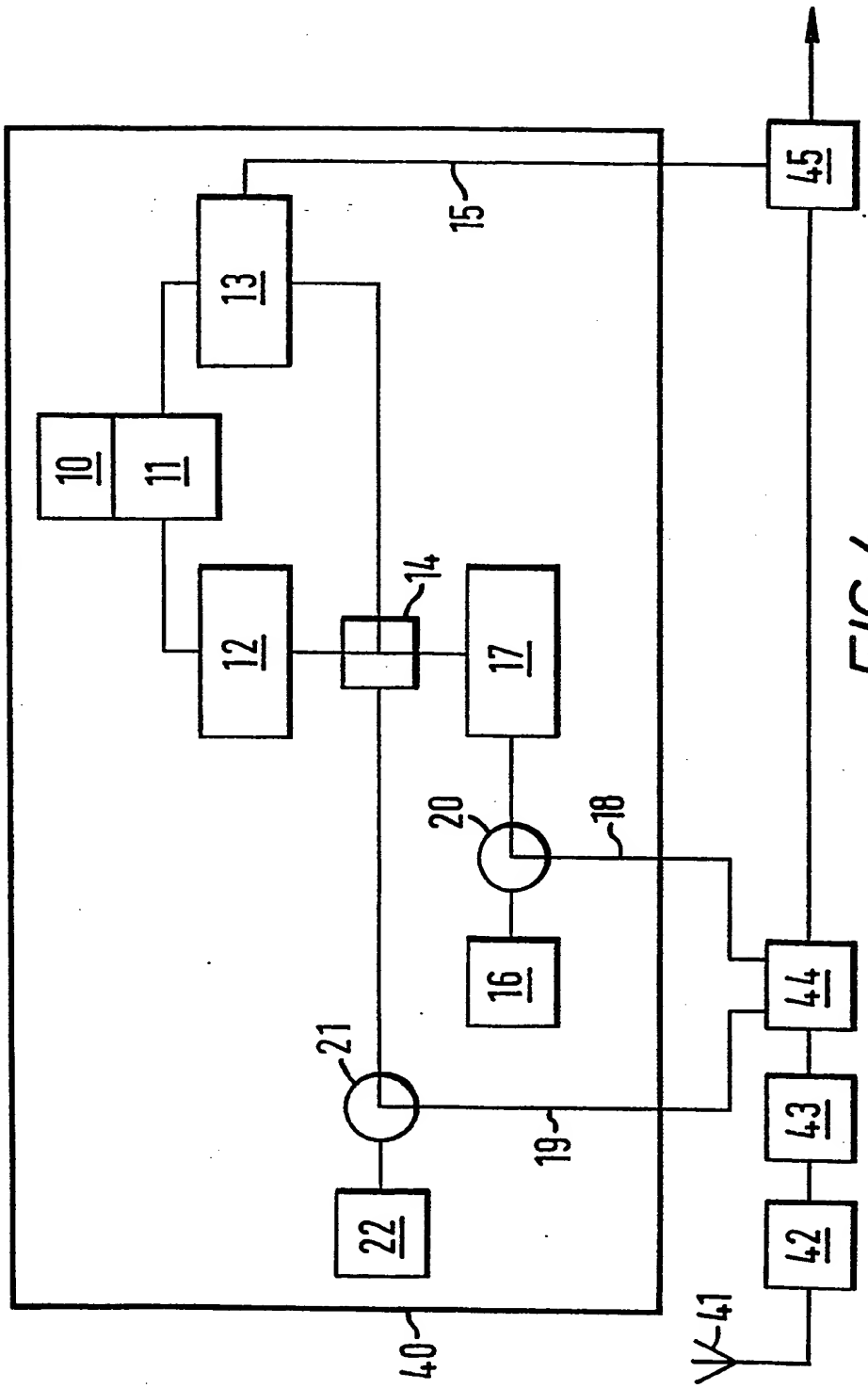

FIG.4

0093525

European Patent Office

EUROPEAN SEARCH REPORT

Application number
EP 83 30 2114

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl. ³)
X	WO-A-8 101 933 (RACAL-MILGO) * Page 9, lines 5-13; page 20, last paragraph - page 21, line 14; page 21, line 24 - page 22, line 8; page 22, lines 22-31; page 26, last paragraph - page 28, line 3; page 28, lines 12-28 *	1-4	H 04 L 9/02 H 04 K 1/02
A	---	6-9	
A	1979 NATIONAL TELECOMMUNICATIONS CONFERENCE RECORD, vol. 3, November 1979, pages 43.5.1 - 43.5.8, New York, USA F.H. MYERS: "A data link encryption system" * Page 43.5.3, left-hand column, lines 1-18; figure 4 *	6-9	
A	---	5	TECHNICAL FIELDS SEARCHED (Int. Cl. ³) H 04 L 9/02 H. 04 L 9/00 H 04 L 9/04 H 04 K 1/02
P,X	US-A-3 291 908 (EHRAT) * Column 2, lines 37-63 *	1,2	

	EP-A-0 073 323 (I.B.M.) * Page 2, line 15 - page 3, line 10; page 4, line 29 - page 5, line 17; page 5, line 34 - page 7, line 18 *		
	--- -/-		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	04-08-1983	HOLPER G.E.E.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO Form 1503. 03.82

European Patent Office

EUROPEAN SEARCH REPORT

Application number

EP 83 30 2114

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl. ³)
A	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 24, no. 8, January 1982, pages 4363-4364, New York, USA J.W. FENNEL et al.: "Clock-protected cryptography" * Page 4363, paragraph 1 *	1	

TECHNICAL FIELDS SEARCHED (Int. Cl. ³)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	04-08-1983	HOLPER G.E.E.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO Form 1503. 03.82